JOURNAL OF ALGEBRA 138, 121–136 (1991)

Primitive Local Galois Representations: An Example

G.-MARTIN CRAM[1]

Institut für Mathematik, Universität Augsburg, Universitätsstraße D-8900 Augsburg, West Germany

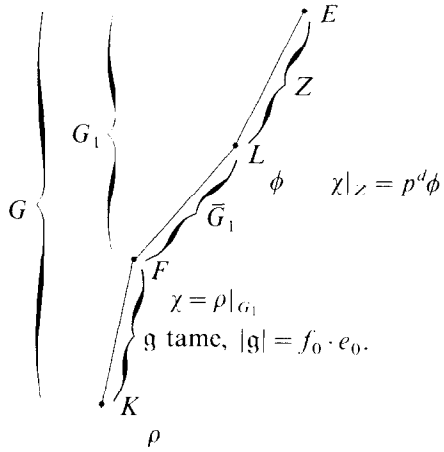
Communicated by A. Fröhlich

Received October 10, 1988

0. INTRODUCTION

The aim of this paper is to study the (Swan) conductor of primitive characters of local Galois groups.

Let $K/\mathbb{Q}_p$ be a p-adic number field, G_K its absolute Galois group, and ρ a primitive, irreducible, complex character of G_K. Let E/K be the fixed field of the kernel of ρ, $G := G_K/\ker \rho = \mathrm{Gal}(E/K)$, and let $E/F/K$ be the field corresponding to the wild ramification subgroup of G, $G_1 := \mathrm{Gal}(E/F)$. Let Z be the center of G_1 and L the corresponding field:



It follows from the work of Koch [4] that

- $\chi := \rho|_{G_1}$ is irreducible,
- Z is central in G,

[1]Present address: Department of Mathematics & Statistics, McMaster University, 1280 Main Street West, Hamilton, Ontario, Canada L8S 4K1.

0021-8693/91 $3.00

— $\chi|_Z = p^d \cdot \phi$, where $\phi \in \operatorname{Irr} Z$ and $p^d = \chi(1)$,

— $\bar{G}_1 := G_1/Z$ is elementary Abelian with order p^{2d},

— the commutator induces a non-degenerate, alternating form

$$\langle\ ,\ \rangle: \bar{G}_1 \times \bar{G}_1 \to \mathbb{C}^*: \langle \bar{x}, \bar{y} \rangle := \phi([x, y]),$$

where $x, y \in G_1$, and $\bar{x}, \bar{y}$ denote their images in $\bar{G}_1$,

— this form is invariant under conjugation with elements of $\mathfrak{g} := \mathrm{Gal}(F/K)$, thus $\bar{G}_1$ becomes a symplectic $\mathbb{F}_p\mathfrak{g}$-module,

— $\bar{G}_1$ is an anisotropic $\mathbb{F}_p\mathfrak{g}$-module; i.e., it has no isotropic submodules.

The character ρ is called "in general position" if its conductor is minimal among the conductors of all twists $\rho\tau$, where τ runs through the one-dimensional characters of G_K.

If ρ is in general position, the Swan conductor of a twist is given by $\mathrm{sw}(\rho\tau) = \min\{\mathrm{sw}(\rho), \rho(1)\,\mathrm{sw}(\tau)\}$; see Lemma 1.6 below. Thus it suffices to determine the conductor of characters in general position.

If the group $\bar{G}_1$ has just one jump at $s = 1$, then Zink has computed the possible values of the conductor of primitive characters [11]. They have the form

$$\mathrm{sw}(\rho) = p^d \cdot \frac{1}{e_0} \cdot s \cdot (1 + p^{-v}), \tag{0.1}$$

where $p^d = \rho(1)$ is the character degree, $e_0 = e(F/K)$ is the tame ramification index of G, s is the jump of $\bar{G}_1$ ($s = 1$ in Zink's work), and v is an integer between 1 and d. Zink associates v with the degree of a polynomial belonging to the symplectic form on $\bar{G}_1$.

The same formula holds for general s if the degree of ρ is $\rho(1) = p$ [1]. In this case $\bar{G}_1$ is irreducible as $\mathbb{F}_p\mathfrak{g}$-module, and since ramification subgroups are invariant, i.e., submodules, $\bar{G}_1$ can have just one jump. Of course $v = 1$ in this case.

The method of Buhler applies to any primitive character ρ if its conductor is prime to p (and $\bar{G}_1$ has just one jump). We get $\mathrm{sw}(\rho) = p^d \cdot (1/e_0) \cdot s \cdot (1 + p^{-d})$ in this case.

Thus we have the question does Zink's formula (0.1) hold in general, i.e., if s is any integer such that $\bar{G}_1$ has just one jump at s? This was asked by Zink [10, 8.4, Bemerkung e].

However, I construct an example where formula (0.1) does not hold. In this example the jump of $\bar{G}_1$ is $s = 2$, the character degree is $\rho(1) = p^2$, and the conductor is $\mathrm{sw}(\rho) = p^2 \cdot (\frac{1}{5}) \cdot (2 + p^{-1})$. p is any prime with $p \equiv 2$

(mod 5), and the ground field is any p-adic number field that contains fifth roots of unity. The tame extension F/K has degree 5 and is totally ramified. The group G_1 is irreducible as $\mathbb{F}_p\mathfrak{g}$-module.

1. Preliminaries

I use the notation in the Introduction. But if I want to talk about general p-adic number fields I use the symbol R for the ground field and ω for a character of its Galois group.

The first six lemmas are either well known or straight forward. But I want to recall them in the form that I need here. Lemmas 1.7 and 1.8 are the crucial points in the construction of the example.

Lemma 1.1. *Let R_2/R_0 be a totally ramified Galois extension of p-adic number fields, $\mathrm{Gal}(R_2/R_1)$ be the wild ramification subgroup, and $\mathfrak{g} = \mathrm{Gal}(R_1/R_0)$ be the tame factor. Set $e_0 := |\mathfrak{g}|$. Let t be any integer, $t \geqq 1$.*

Then $U^t_{R_2}/U^{t+1}_{R_2}$ is a homogeneous $\mathbb{F}_p\mathfrak{g}$-module, i.e., isomorphic to several copies of one irreducible module V. To determine V, choose $\sigma \in \mathrm{Gal}(R_2/R_0)$ such that its image in $\mathfrak{g}$ generates $\mathfrak{g}$, and choose a prime element π of R_2.

Then $\pi^{\sigma-1} \equiv \omega \pmod{U^1_{R_2}}$, where ω is a primitive e_0th root of unity, and V can be identified with $\mathbb{F}_p(\omega^t)$, where σ acts by multiplication with ω^t.

Notation. $V = (\mathbb{F}_p(\omega^t),\ \sigma \to \omega^t)$.

Proof. For any $\tau \in \mathrm{Gal}(R_2/R_0)$ and $x = 1 + \pi^t\varepsilon \in U^t_{R_2}$, $x^{\tau-1} \equiv 1 + \pi^t \cdot (\pi^{\tau-1})^t \cdot \varepsilon \pmod{U^{t+1}_{R_2}}$. Thus the wild ramification subgroup acts trivial, and under the isomorphism

$$U^t_{R_2}/U^{t+1}_{R_2} \to \bar{R}_2 = \bar{R}_0$$
$$1 + \pi^t\varepsilon \to \bar{\varepsilon},$$

we can identify $U^t_{R_2}/U^{t+1}_{R_2}$ with a field extension of $\mathbb{F}_p$, where σ acts by multiplication with ω^t. That ω is a root of unity follows from the structure of the units of R_2 (see [2, Chap. 15]). Q.E.D.

Lemma 1.2. *Let ω be an irreducible complex character of the absolute Galois group G_R of the p-adic number field R. Then the Swan conductor of ω is given by*

$$\mathrm{sw}(\omega) = \omega(1) \cdot j,$$

where j is the largest index in the upper numbering of the ramification subgroups of G_R such that G^j_R is not contained in the kernel of ω.

Proof [6, Chap. VI, Sect. 2, Exercise 2]. Serre considers the Artin conductor $\mathrm{ar}(\omega)$. For an irreducible character ω, $\omega \neq 1$, the Swan conductor is defined by $\mathrm{sw}(\omega) = \mathrm{ar}(\omega) - \omega(1)$. Q.E.D.

LEMMA 1.3. *Using the notation in the Introduction, we have*

(i) $\mathrm{sw}(\rho) = (1/e_0)\,\mathrm{sw}(\chi)$,

(ii) *ρ is in general position iff χ is in general position.*

Proof. (i) follows from Lemma 1.2, as does (ii) "$\Rightarrow$". For "$\Leftarrow$" one must show that if $\chi\tau$ is in general position, with a one-dimensional character τ of G_F, then there exists a one-dimensional character τ' of G_K such that $\mathrm{sw}(\chi\tau) = \mathrm{sw}(\rho\tau' | G_F)$. The proof follows the idea of Buhler [1, Claim 1, p. 28]; see also Henniart [3, Theorems 1.7 and 5.3]. Q.E.D.

LEMMA 1.4. *Using the notation in the Introduction, if $\bar{G}_1$ has just one jump at s, then the conductor of ρ is of the form*

$$\mathrm{sw}(\rho) = \rho(1) \cdot \frac{1}{e_0} \cdot (s + a \cdot p^{\,v}),$$

with integers a and v such that $1 \leqq v \leqq d$, $1 \leqq a \leqq s$, and $\gcd(a, p) = 1$.

Proof [10, Proposition 8.4]. (Zink computes the possible values of $\mathrm{sw}(\chi)/\chi(1)$. Apply Lemmas 1.2 and 1.3 to Zink's formula.) Q.E.D.

Remark. The nature of v and a is not yet understood. Zink asked whether we always have $a = s$, but this is false, as the example shows.

LEMMA 1.5. *Let $L/F/K$ be Galois extensions of the p-adic number field K, let F/K be tamely, and let L/F be totally and wildly ramified with $\bar{G}_1 := \mathrm{Gal}(L/F)$ elementary Abelian.*

Assume that $\langle\ ,\ \rangle\colon \bar{G}_1 \times \bar{G}_1 \to \mathbb{C}^*$ is a non-degenerate, alternating form, invariant under $\mathfrak{g} := \mathrm{Gal}(F/K)$.

(i) *If $p \neq 2$, there exists a projective, irreducible representation $\bar{\rho}$ of G_K with kernel $\geqq G_L$ such that its restriction $\bar{\chi} := \bar{\rho}|_{G_F}$ remains irreducible and such that it induces the given form.*

Let ρ be any ordinary, complex character that lifts $\bar{\rho}$, and let $\rho|_{G_L} = \rho(1) \cdot \phi$, with ϕ a one-dimensional character of G_L. Then

$$\langle \bar{x}, \bar{y} \rangle = \phi([x, y]) \qquad \text{for} \quad x, y \in G_F,$$

where $\bar{x}$, $\bar{y}$ denote their images in $\bar{G}_1$.

(ii) *The character ρ of* (i) *is primitive iff the $\mathbb{F}_p\mathfrak{g}$-module $\bar{G}_1$ is anisotropic. In this case the projective representation $\bar{\rho}$ is unique.* (*And it exists even if $p=2$.*)

(iii) *The projective representation $\bar{\rho}$ of* (i) *is also unique if $|\mathfrak{g}|$ is prime to p, in particular if $|\mathfrak{g}|=1$, i.e., $F=K$.*

Proof. (i) [9, Satz 5]. (Note that any projective representation is liftable, since $H^2(G_K, \mathbb{C}^*)=0$; see [5, Part II].)

(ii) [9, Satz 6].

(iii) [9, Satz 3 (II)]. Q.E.D.

Lemma 1.5 allows us to define the conductor of an alternating form:

DEFINITION. Let L/F be an elementary Abelian and a totally and wildly ramified extension. Let

$$X: \mathrm{Gal}(L/F)\times\mathrm{Gal}(L/F)\to\mathbb{C}^*$$

be an alternating form. Define $j(X)$ as the minimum of $\mathrm{sw}(\chi)/\chi(1)$, where χ runs through the lifts of the projective representation $\bar{\chi}$ of G_F defined by X.

(To define $j(X)$ one just needs L/F to be Abelian; see [11]. But I just need those forms in the definition above.)

The next two lemmas give a simple observation about the conductor of the product of characters resp. forms:

LEMMA 1.6. *Let ω_1, ω_2 be two irreducible characters of the absolute Galois group of the p-adic field R such that $\omega_1\cdot\omega_2$ is irreducible too. Then*

$$\frac{\mathrm{sw}(\omega_1\cdot\omega_2)}{\omega_1(1)\cdot\omega_2(1)}\leqq\max\left\{\frac{\mathrm{sw}(\omega_1)}{\omega_1(1)},\frac{\mathrm{sw}(\omega_2)}{\omega_2(1)}\right\}.$$

And if $\mathrm{sw}(w_1)/\omega_1(1)\neq\mathrm{sw}(\omega_2)/\omega_2(1)$, we have equality in the formula above.

Proof. Use Lemma 1.2. Q.E.D.

LEMMA 1.7. *Let L/F be an elementary Abelian and a totally and wildly ramified extension of p-adic number fields, and let X_1, X_2 be two alternating forms on* $\mathrm{Gal}(L/F)$. *Then*

$$j(X_1\cdot X_2)\leqq\max\{j(X_1), j(X_2)\}.$$

And if $j(X_1)\neq j(X_2)$, equality holds in the formula above.

Proof. Set $X_3 := X_1 \cdot X_2$. Choose characters χ_1, χ_2, χ_3 of G_F such that χ_i belongs to X_i (in the sense of Lemma 1.5) and such that $j(X_i) = \mathrm{sw}(\chi_i)/\chi_i(1)$. "Belonging to X_i" means that $\chi_i|_{G_L} = \chi_i(1) \cdot \phi_i$, where ϕ_i is a one-dimensional character of G_L such that for $x, y \in G_F$,

$$X_i(\bar{x}, \bar{y}) = \phi_i([x, y]).$$

Hence

$$\phi_3|_{[G_F, G_F]} = \phi_1 \cdot \phi_2|_{[G_F, G_F]},$$

and thus

$$\phi_3 = \phi_1 \cdot \phi_2 \cdot \tau, \tag{*}$$

where τ is a one-dimensional character of G_L that is trivial on $[G_F, G_F]$.

Claim 1. $j_i := j(X_i) \overset{!}{=} \Phi_{L/F}(\mathrm{sw}(\phi_i))$, where $\Phi_{L/F}$ denotes the Herbrand function of L/F.

Proof of Claim 1. By Lemma 1.2, $G_F^{j_i} \not\leqq \ker \chi_i$, but for any $\varepsilon > 0$, $G_F^{j_i + \varepsilon} \leqq \ker \chi_i$. It follows that $G_F^{j_i + \varepsilon} \cap G_L \leqq \ker \phi_i$, and the claim asserts that $G_F^{j_i} \cap G_L \not\leqq \ker \phi_i$. Assume to the contrary that $G_F^{j_i} \cap G_L \leqq \ker \phi_i$. Then $G_F^{j_i} \cdot G_L$ is contained in the radical of X_i, because for $x \in G_F^{j_i}$ and $y \in G_F$, $[x, y] \in G_F^{j_i} \cap G_L$, and thus $X_i(\bar{x}, \bar{y}) = \phi_i([x, y]) = 1$. Now extend ϕ_i to a character $\tilde{\phi}_i$ of $G_F^{j_i} \cdot G_L$ such that $G_F^{j_i} \leqq \ker \tilde{\phi}_i$. The form X_i is also defined by $\tilde{\phi}_i$. Take any irreducible character $\tilde{\chi}_i$ of G_F lying over $\tilde{\phi}_i$. Then $\tilde{\chi}_i$ belongs to X_i, but $G_F^{j_i} \leqq \ker \tilde{\chi}_i$. This contradicts the minimality of $\mathrm{sw}(\chi_i)/\chi_i(1)$. Claim 1 follows.

The lemma now follows from

Claim 2. $\mathrm{sw}(\phi_3) \leqq \max\{\mathrm{sw}(\phi_1), \mathrm{sw}(\phi_2)\}$, with equality if $\mathrm{sw}(\phi_1) \neq \mathrm{sw}(\phi_2)$.

Proof of Claim 2. The form X_3 is defined by $\phi_1 \cdot \phi_2$. Since $\mathrm{sw}(\chi_3)/\chi_3(1)$ is chosen minimal, we get (by Claim 1 and Lemma 1.6)

$$\mathrm{sw}(\phi_3) \leqq \mathrm{sw}(\phi_1 \cdot \phi_2) \leqq \max\{\mathrm{sw}(\phi_1), \mathrm{sw}(\phi_2)\}. \tag{**}$$

Now consider the case $\mathrm{sw}(\phi_1) > \mathrm{sw}(\phi_2)$. By (*) and Lemma 1.6,

$$\mathrm{sw}(\phi_3) \leqq \max\{\mathrm{sw}(\phi_1 \cdot \tau), \mathrm{sw}(\phi_2)\}.$$

By the choice of χ_1 (and Claim 1) we know that $\mathrm{sw}(\phi_1 \cdot \tau) \geqq \mathrm{sw}(\phi_1)$. Thus by Lemma 1.6, $\mathrm{sw}(\phi_3) = \mathrm{sw}(\phi_1 \cdot \tau) \geqq \mathrm{sw}(\phi_1)$. Together with (**) this yields the equality. Q.E.D.

The following lemma is a variation of a result of Zink. I need some

Notation. If L/F is a Galois extension and $U \leqq L^*$ a subgroup of the multiplicative group of L, set

$$J_F U := \langle u^{\sigma-1} / u \in U, \sigma \in \mathrm{Gal}(L/F) \rangle.$$

LEMMA 1.8. *Let L/F be an Abelian extension of p-adic number fields such that* $\mathrm{Gal}(L/F)$ *has just one jump at s, $s \geqq 1$, $p \nmid s$. Let t be an integer with $t > s$. On $J_F U_L^t / J_F U_L^{t+1}$ consider the filtration*

$$V^j := (U_L^j \cap J_F U_L^t) \cdot J_F U_L^{t+1} / J_F U_L^{t+1}, \qquad j = 0, 1, \ldots.$$

The jumps *of this filtration occur at the indices*

$$j_\nu := t + p^\nu \cdot s, \qquad \nu = 0, \ldots, \min\{m-1, w-\delta\},$$

where m, w, and δ are defined as

$$p^m := |L:F|,\ w := \textit{p-value of } (t-s), \textit{ and if } s + (t-s)/p^w \equiv 0 \pmod{p}, \textit{ then } \delta := 1; \textit{ otherwise } \delta := 0.$$

Moreover the order *of the jumps is $|V^{j_\nu} : V^{j_\nu+1}| = q := |\bar{F}|$, where $\bar{F}$ denotes the residue class field.*

Remarks. (1) Zink considers the case $t = s$ [10, Proposition 8.5]. The proof is similar but differs in some technical details. The result for $t = s$ is more complicated.

(2) I need this lemma with $m = 2d$, $s = 1$, $t = \Psi_{L/F}(2) = 1 + p^{2d}$. In this case $w = m = 2d$ and $\delta = 0$.

Proof.

Claim 1. If $p \mid t$, then $J_F U_L^t = J_F U_L^{t+1}$.

Let $x \in U_L^t$ and $\sigma \in \mathrm{Gal}(L/F)$. To show that $x^{\sigma-1} \in (U_L^{t+1})^{\sigma-1}$, choose a prime element π_σ of the fixed field of σ, and write

$$x = (1 + \pi_\sigma^{t/p} \cdot \omega) \cdot x_1,$$

where ω is a p-regular root of unity (and thus in F) and where $x_1 \in U_L^{t+1}$. It follows that $x^{\sigma-1} = x_1^{\sigma-1}$.

Claim 2. Assume that $p \nmid t$. Then the first jump is $j_0 = s + t$, and its order is q.

From [6, Chap. IV, Sect. 2, Exercise 3a], for $x = 1 + y \in U_L^t$ and $\sigma \in \mathrm{Gal}(L/F)$, $\sigma \neq 1$ (and π a prime element of L) follows:

$$x^{\sigma-1} \equiv 1 + t \cdot (\pi^{\sigma-1} - 1) \cdot y \pmod{U_L^{s+t+1}}.$$

Thus $J_F U_L^t \leqq U_L^{s+t}$, and analogously $J_F U_L^{t+1} \leqq U_L^{s+t+1}$; moreover, for fixed σ, $\sigma \neq 1$, we get an isomorphism:

$$(U_L^t)^{\sigma-1}/(U_L^{t+1})^{\sigma-1} \xrightarrow{\sim} U_L^{s+t}/U_L^{s+t+1}. \qquad (***)$$

Hence the first jump is indeed j_0, and its order is given by

$$|J_F U_L^t : (J_F U_L^t \cap U_L^{s+t+1}| = |U_L^{s+t} : U_L^{s+t+1}|.$$

Claim 3. Assume that $p \nmid t$ and $|L:F| = p$. Then j_0 is the only jump.

This follows because $\mathrm{Gal}(L/F)$ is cyclic, thus $J_F U_L^t = (U_L^t)^{\sigma-1}$ for a generator σ of $\mathrm{Gal}(L/F)$. Now look at $(***)$ in the proof of Claim 2.

Claim 4. Assume that $p \nmid t$. The lemma follows by induction on m.

After Claim 3 we are left with the case $m > 1$. Choose an intermediate field $L/L'/F$ with $|L:L'| = p$. Consider the following sequences for $j \geqq s+t+1$:

$$U_L^j \cap J_{L'} L^* \rightarrowtail U_L^j \cap J_F U_L^t \xrightarrow{N_{L/L'}} U_{L'}^{\Phi_{L/L'}(j)} \cap J_F U_{L'}^{\Phi_{L/L'}(t)},$$

$$U_L^j \cap J_{L'} L^* \rightarrowtail U_L^j \cap J_F U_L^{t+1} \xrightarrow{N_{L/L'}} U_{L'}^{\Phi_{L/L'}(j)} \cap J_F U_{L'}^{\Phi_{L/L'}(t+1)}.$$

These sequences are exact. It suffices to consider the first one:

Surjectivity of the Norm. We have $N_{L/L'}(J_F U_L^t) = J_F(N_{L/L'} U_L^t) = J_F U_{L'}^{\Phi_{L/L'}(t)}$ and $N_{L/L'}(U_L^j) = U_{L'}^{\Phi_{L/L'}(j)}$, since j and t are greater then the jump s of L/L'; see [6, Chap. V, Sect. 6, Corollary 4 to Proposition 9]. Let $r \in U_{L'}^{\Phi_{L/L'}(j)} \cap J_F U_{L'}^{\Phi_{L/L'}(t)}$ with

$$r = N_{L/L'}(x), \qquad x \in U_L^j,$$

and

$$r = N_{L/L'}(y), \qquad y \in J_F U_L^t.$$

Then

$$\begin{aligned} h := xy^{-1} &\in \ker(N_{L/L'}) \cap U_L^j \cdot J_F U_L^t \\ &= J_{L'} L^* \cap U_L^j \cdot J_F U_L^t \qquad \text{(since } L/L' \text{ is cyclic)} \\ &\leqq J_{L'} L^* \cap U_L^{s+t} \qquad \text{(Claim 4).} \end{aligned}$$

But $J_{L'} L^* = (L^*)^{\sigma-1}$ for a generator σ of $\mathrm{Gal}(L/L')$, and $(L^*)^{\sigma-1} \cap U_L^{s+t} = (U_L^t)^{\sigma-1}$. This follows again from [6, Chap. IV, Sect. 2, Exercise 3a]. Thus $h \in (U_L^t)^{\sigma-1} \leqq J_F U_L^t$, and hence $x = yh \in J_F U_L^t \cap U_L^j$.

Exactness in the Middle. The kernel of the norm is

$$\begin{aligned} U_L^j \cap J_F U_L^t \cap \ker(N_{L/L'}) &= U_L^j \cap J_F U_L^t \cap J_{L'} L^* \\ &= U_L^j \cap J_F U_L^t \cap J_{L'} U_L^t \\ &\qquad \text{(since } U_L^j \text{ and } J_F U_L^t \text{ are in } U_L^{s+t}\text{)} \\ &= U_L^j \cap J_{L'} U_L^t = U_L^j \cap J_{L'} L^*. \end{aligned}$$

Consider the cokernel of the embedding of the second sequence into the first one. This yields an isomorphism:

$$\frac{U_L^j \cap J_F U_L^t}{U_L^j \cap J_F U_L^{t+1}} \xrightarrow[\simeq]{N_{L/L'}} \frac{U_{L'}^{\Phi_{L/L'}(j)} \cap J_F U_{L'}^{\Phi_{L/L'}(t)}}{U_{L'}^{\Phi_{L/L'}(j)} \cap J_F U_{L'}^{\Phi_{L/L'}(t+1)}}. \qquad (****)$$

Thus apart from the jump j_0, the jumps of $J_F U_L^t / J_F U_L^{t+1}$ are determined by the right side of (****). We have $\Phi_{L/L'}(t) = s + (t-s)/p$. If $t \not\equiv s \pmod p$, then $\Phi_{L/L'}(t)$ is not an integer, and the right side of (****) vanishes. If $t \equiv s \pmod p$, but $\Phi_{L/L'}(t) \equiv 0 \pmod p$, the right side vanishes too (Claim 3). In all other cases the jumps of the right side are given by induction: Let $|L' : F| = p^{m'}$ with $m' = m - 1$. $\mathrm{Gal}(L'/F)$ has just one jump at s. Set $t' := \Phi_{L/L'}(t)$. The p-value of $(t' - s)$ is $w' = w - 1$, and the summand δ is the same as before. Thus the jumps of the right side are given by

$$j'_\nu = t' + p^\nu \cdot s, \qquad \nu = 0, \ldots, \min\{m' - 1, w' - \delta\},$$

and the order of all jumps is q.

Hence $J_F U_L^t / J_F U_L^{t+1}$ has the jump j_0 and the jumps

$$\Psi_{L/L'}(j'_\nu) = t + p^{\nu+1} \cdot s, \qquad \nu + 1 = 1, \ldots, \min\{m - 1, w - \delta\}.$$

$\Psi_{L/L'}$ denotes the inverse of the Herbrand function $\Phi_{L/L'}$. Q.E.D.

2. Example

In the notation of the introduction choose an odd prime p such that $p \equiv 2 \pmod 5$. As ground field choose a p-adic number field that contains fifth roots of unity. Let F/K be a totally and tamely ramified Galois extension of degree $e_0 := 5$. To do this, choose a prime element π_K of K and set $\pi_F := \sqrt[5]{\pi_K}$. Then $F = K(\pi_F)$ and π_F is a prime element of F. $\mathfrak{g} := \mathrm{Gal}(F/K) = \langle \sigma \rangle$ with $\pi_F^\sigma = \alpha \cdot \pi_F$, where α is a primitive fifth root of unity in K.

PROPOSITION 2.1. *There exists a primitive character ρ of G_K with the following properties:*

(i) *Let E be the fixed field of the kernel of ρ. Then E is a totally and wildly ramified extension of F.*

(ii) *Let $Z = \mathrm{Gal}(E/L)$ be the center of $\mathrm{Gal}(E/K)$. Then L is an extension of F, and $\bar{G}_1 := \mathrm{Gal}(L/F)$ is a chief factor of $\mathrm{Gal}(L/K)$, i.e., $\bar{G}_1$ is an irreducible $\mathbb{F}_p\mathfrak{g}$-module.*

(iii) $p^d := \rho(1) = p^2$.

(iv) *$\bar{G}_1$ has just one jump at $s = 2$.*

(v) *ρ is in general position.*

But

(vi) $\mathrm{sw}(\rho) = p^d \cdot (1/e_0) \cdot (2 + p^{-1}) = p \cdot (2p + 1)/5$.

Remark 2.2. There also exist primitive characters ρ' satisfying conditions (i)–(v), but whose conductor is prime to p; i.e.,

$$\mathrm{sw}(\rho') = p^d \cdot \frac{1}{e_0} \cdot (2 + 2 \cdot p^{-d}) = \frac{2(p^2 + 1)}{5}.$$

After the proof of Proposition 2.1 I sketch the proof of the remark.

Proof. If ρ' is any primitive character satisfying (i)–(v), then by Lemma 1.4 the conductor has the form

$$\mathrm{sw}(\rho') = p^d \cdot \frac{1}{e_0} \cdot (s + a \cdot p^{-v}),$$

$$\text{with } 1 \leqq a \leqq s = 2 \text{ and } 1 \leqq v \leqq d = 2.$$

But $\mathrm{sw}(\rho')$ is an integer! Hence there are only two possibilities:

(I) $v = 2$ and $a = 2$: $\mathrm{sw}(\rho') = p^d \cdot (1/e_0) \cdot (s + s \cdot p^{-2})$,

(II) $v = 1$ and $a = 1$: $\mathrm{sw}(\rho') = p^d \cdot (1/e_0) \cdot (s + 1 \cdot p^{-1})$.

I must show that the second possibility does occur!

Step 1. I construct a primitive character ρ' satisfying (i)–(v): Consider U_F^2/U_F^3 as $\mathbb{F}_p\mathfrak{g}$-module. By Lemma 1.1 it is homogenous with irreducible submodule $V = (\mathbb{F}_p(\alpha^2),\ \sigma \to \alpha^2)$. Since e_0 is odd, $\mathbb{F}_p(\alpha^2) = \mathbb{F}_p(\alpha)$, and $\dim_{\mathbb{F}_p} V = 2d = 4$.

Now we need an alternating form on V. I write forms multiplicatively, but the description of the forms on V is better done additively. Thus let me fix

once and for all an embedding $\mathbb{F}_p^+ \to \mathbb{C}^*$. The $\mathfrak{g}$-invariant, alternating forms on V are given as follows: Let $\phi_0 \in \mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ with $\mathrm{ord}\,\phi_0 = 2$. Then every $\mathfrak{g}$-invariant form Y is given by an element $v_0 \in \mathbb{F}_p(\alpha)$ with $\phi_0(v_0) = -v_0$:

$$Y(v, w) = \operatorname{tr}_{\mathbb{F}_p(\alpha)/\mathbb{F}_p}(v_0 \cdot v \cdot \phi_0(w)) \to \mathbb{C}^*.$$

Here $\operatorname{tr}_{\mathbb{F}_p(\alpha)/\mathbb{F}_p}$ dentoes the trace. This form is $\mathfrak{g}$-invariant since $\phi_0(\alpha) = \alpha^p = \alpha^{-1}$; see [7, Theorem 3.1]. Choose a $\mathfrak{g}$-invariant subgroup N^2, $U_F^3 \leqq N^2 \leqq U_F^2$, such that $U_F^2/N^2 \simeq V$ as $\mathbb{F}_p\mathfrak{g}$-module. Further choose a $\mathfrak{g}$-invariant subgroup $N' \leqq F^*$ such that $U_F^2 \cdot N' = F^*$ and $U_F^2 \cap N' = N^2$. Let L'/F be the Abelian extension such that $N_{L'/F}L'^* = N'$ (this is local class field theory; see [6, Chap. XIV, Sect. 6, Theorem 1]):

$$V \simeq \begin{cases} U_F^2 \\ N^2 \\ U_F^3 \end{cases} \begin{array}{l} \\ \\ \\ \end{array} \begin{array}{l} F^* \\ N' = N_{L'/F}L'^* \\ \\ \end{array}$$

Hence $\mathrm{Gal}(L'/F) \simeq V$ as $\mathbb{F}_p\mathfrak{g}$-module and $\mathrm{Gal}(L'/F)$ has a $\mathfrak{g}$-invariant, alternating form X'.

By Lemma 1.5 there exists a projective representation $\bar{\rho}'$ of G_K belonging to the form X', and a suitable lifting of $\bar{\rho}'$ gives us a primitive character ρ' that satisfies (i)–(v), with L' as the fixed field of the center of $G_K/\ker \rho'$.

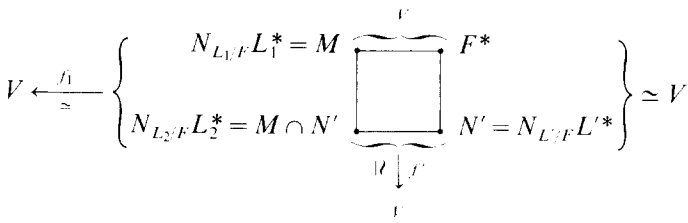
Step 2. As remarked at the beginning of the proof, there are two possibilities for $\mathrm{sw}(\rho')$. If $\mathrm{sw}(\rho') = p^2 \cdot \frac{1}{5} \cdot (2 + p^{-1})$, we are done. Thus let us assume that this is not the case. Then $\mathrm{sw}(\rho') = p^2 \cdot \frac{1}{5} \cdot (2 + 2 \cdot p^{-2})$, and I must construct a new character ρ.

The center of ρ will belong to a new field L/F. To find this field, consider U_F^1/U_F^2 as $\mathbb{F}_p\mathfrak{g}$-module. By Lemma 1.1 it is homogeneous with irreducible submodule $(\mathbb{F}_p(\alpha), \sigma \to \alpha)$. But since $p \equiv 2 \pmod{e_0}$, the map

$$(\mathbb{F}_p(\alpha), \sigma \to \alpha) \to (\mathbb{F}_p(\alpha), \sigma \to \alpha^2) = V$$
$$x \longrightarrow x^p$$

is an $\mathbb{F}_p\mathfrak{g}$-module isomorphism.

Choose a $\mathfrak{g}$-invariant subgroup N^1, $U_F^2 \leqq N^1 \leqq U_F^1$, and a $\mathfrak{g}$-invariant subgroup M with $U_F^1 \cdot M = F^*$ and $U_F^1 \cap M = N^1$. Let L_1/F be the Abelian extension with $N_{L_1/F}L_1^* = M$, and let L_2/F be that extension with $N_{L_2/F}L_2^* = M \cap N'$:



Fix isomorphisms

$$f_1 : \mathrm{Gal}(L_2/L_1) \xrightarrow{\sim} V, \qquad f' : \mathrm{Gal}(L_2/L') \xrightarrow{\sim} V,$$

and

$$f_1 \oplus f' : \mathrm{Gal}(L_2/F) \xrightarrow{\sim} V \oplus V.$$

Fix a $\mathfrak{g}$-invariant, alternating form Y on V that corresponds to the form X' under $\mathrm{Gal}(L'/F) \xrightarrow{\sim} \mathrm{Gal}(L_2/L_1) \xrightarrow{f_1} V$. On $V \oplus V$ we get the non-degenerate form

$$Y \times Y : (V \oplus V) \times (V \oplus V) \to \mathbb{C}^*$$
$$(v_1 \oplus w_1, v_2 \oplus w_2) \to Y(v_1, v_2) \cdot Y(w_1, w_2).$$

We also have the form $Y \times 1$ with radical $0 \oplus V$,

$$Y \times 1 : (V \oplus V) \times (V \oplus V) \to \mathbb{C}^*$$
$$(v_1 \oplus w_1, v_2 \oplus w_2) \to Y(v_1, v_2),$$

and similarly the form $1 \times Y$ with radical $V \oplus 0$.

To construct the form that will belong to the character ρ, consider the diagonal

$$D^+ := \{v \oplus v / v \in V\}$$

and the "anti-diagonal"

$$D^- := \{v \oplus (-v) / v \in V\}.$$

The form $Y \times Y$ is non-degenerate on both diagonals, and they are orthogonal to each other with respect to this form.

I want to construct two forms Y_+ and Y_- with radicals D^+ and D^-, resp., such that $Y_+|_{D^- \times D^-} = Y \times Y|_{D^- \times D^-}$, and similarly for Y_-. This is done by setting

$$Y_+(v_1 \oplus w_1, v_2 \oplus w_2) := Y(v_1 - w_1, v_2 - w_2)^{1/2}.$$

Note that the square root is unique within pth roots of unity.

The form that defines the character ρ will correspond to Y_+^2. Read all these forms on $\mathrm{Gal}(L_2/F)$ by the fixed isomorphism. Let $\mathrm{Gal}(L_2/L) \leq \mathrm{Gal}(L_2/F)$ be the group corresponding to D^+, and denote by X the form on $\mathrm{Gal}(L/F)$ corresponding to the form Y_+^2 on $(V \oplus V)/D^+$. By Lemma 1.5 we get a primitive character ρ that satisfies (i)–(v).

Step 3. It remains to compute the conductor of ρ.

Lemma 1.3 reduces this problem to the conductor $\chi := \rho|_{G_F}$, and by Lemma 1.5 we can translate this into the conductor of the form X.

Let X_2 be the form on $\mathrm{Gal}(L_2/F)$ that corresponds to $Y \times Y$ on $V \oplus V$, let X_1 correspond to $1 \times Y$, and let X' correspond to $Y \times 1$. Then $X_2 = X_1 \cdot X'$ with conductors

$$j(X') = 2 + 2 \cdot p^{-2} \qquad \text{by assumption on } \mathrm{sw}(\rho'),$$

and

$$j(X_1) = 1 + 1 \cdot p^{-1} \text{ (By Lemma 1.4,} \qquad j(X_1) = 1 + p^{-v}, \text{ with } v = 1, 2.$$

But X_1 is g-invariant, thus the conductor of ρ_1 of G_K belonging to X_1 is an integer. Hence $j(X_1)$ is "divisible" by $e_0 = 5$.) Hence Lemma 1.7 implies that

$$j(X_2) = 2 + 2 \cdot p^{-2}.$$

Define a form Z on $\mathrm{Gal}(L_2/F)$ by

$$X_2 = X \cdot Z.$$

I show that $j(Z) > j(X_2)$. Then by Lemma 1.7, $j(X) = j(Z)$.

It remains to prove the following

Claim. $j(Z) = 2 + p^{-1}$.

Thus let us study the form Z:

$$\mathrm{Gal}(L_2/L_1) \text{ is isotropic for } Z. \tag{*1}$$

This I compute on $V \oplus V$. Restrict $Y \times Y = Y_+^2 \cdot Z$ to $(V \oplus 0) \times (V \oplus 0)$:

$$Y_+^2(v_1 \oplus 0, v_2 \oplus 0) = Y(v_1, v_2) = Y \times Y(v_1 \oplus 0, v_2 \oplus 0).$$

Thus $Z(v_1 \oplus 0, v_2 \oplus 0) = 1$.

It follows that there exists a one-dimensional character θ of G_{L_1} that defines Z: By Lemma 1.5 we get a character χ_Z of G_F with $\chi_Z|_{G_{L_2}} = \chi_Z(1) \cdot \phi_Z$, and ϕ_Z defines Z. But G_{L_1} is isotropic for Z; this means that $G_{L_1}/\ker \phi_Z$ is Abelian, and thus ϕ_Z is extendible to θ on G_{L_1}.

Choose θ such that its conductor is minimal. Then

$$j(Z) = \Phi_{L_1/F}(\mathrm{sw}(\theta)). \qquad (*2)$$

This follows by the same argument as the Claim 1 in the proof of Lemma 1.7. It remains to show that

Claim'. $\mathrm{sw}(\theta) \overset{!}{=} \Psi_{L_1/F}(2 + p^{-1}) = 1 + p^4(1 + p^{-1}) = 1 + p^4 + p^3$. ($\Psi_{L_1/F}$ denotes the inverse of the Herbrand function. Note that $|L_1/F| = p^4$ and that L_1/F has just one jump at $s_1 = 1$.)

Translate the problem into the relative Weil group $W := W_{L_1/F}$:

$$\begin{array}{ccccc}
L_1^* & \rightarrowtail & W & \twoheadrightarrow & \mathrm{Gal}(L_1/F) \\
\downarrow & & \downarrow & & \| \\
G_{L_1}^{ab} & \rightarrowtail & G_F/G'_{L_1} & \twoheadrightarrow & \mathrm{Gal}(L_1/F) \\
\| & & & & \\
G_{L_1}/G'_{L_1} & & & &
\end{array}$$

(W is the Weilgroup of L_1^{ab}/F, a subgroup of $\mathrm{Gal}(L_1^{ab}/F) = G_F/G'_{L_1}$. See [8, Appendices II and III.) Then Z becomes a $\mathfrak{g}$-invariant form on W, θ a character of L_1^*, and

$$Z(x, y) = \theta([x, y]) \qquad \text{for} \quad x, y \in W.$$

The relative Weil group is the context in which to formulate the next two facts:

$$U_{L_1}^{\Psi_{L_1/F}(2)+1} \text{ is contained in the radical of } Z. \qquad (*3)$$

This follows since $N_{L_1/F}(U_{L_1}^{\Psi_{L_1/F}(2)+1}) = U_F^3 \leqq M \cap N'$; see [6, Chap. V, Sect. 6, Corollary 4 to Proposition 9]. But $M \cap N' = N_{L_2/F}(L_2^*)$ is contained in the radical of Z. Here I identified $F^*/M \cap N'$ with $\mathrm{Gal}(L_2/F)$ by local class field theory.

$$U_{L_1}^{\Psi_{L_1/F}(2)} \text{ is not contained in the radical of } Z. \qquad (*4)$$

Assume that (*4) is false. Again read Z as a form on F^* by class field theory. Then $N_{L_1/F}(U_{L_1}^{\Psi_{L_1/F}(2)}) = U_F^2$ is contained in the radical of Z (again see [6, Chap. V, Sect. 6, Corollary 4 to Proposition 9]). But also $M \cap N' \leqq \mathrm{rad}\, Z$. Thus $U_F^2 \cdot (M \cap N') = M \leqq \mathrm{rad}\, Z$. Now transport this problem to $V \oplus V$. Then $Y \times Y = Y_+^2 \cdot Z$ and $V \oplus 0 \leqq \mathrm{rad}\, Z$, $D^+ \leqq \mathrm{rad}\, Y_+^2$. This implies that $V \oplus 0$ and D^+ are orthogonal to each other (with respect to

$Y \times Y$). But this is nonsense: The orthogonal complement of $V \oplus 0$ is $0 \oplus V$ and that of D^+ is D^-.

Translate (*3) and (*4) into a fact about θ. Restrict θ to $[U_{L_1}^{\Psi_{L_1/F}(2)}, W] = J_F U_{L_1}^{\Psi_{L_1/F}(2)}$: This restriction is not trivial by (*4), but $J_F U_{L_1}^{\Psi_{L_1/F}(2)+1}$ is contained in the kernel of θ by (*3). Set $t := \Psi_{L_1/F}(2) = 1 + p^4$. It follows from Lemma 1.8 (with $s = 1$) that $\theta|_{J_F U_{L_1}^t}$ has a "conductor" of the form $j_v = t + p^v \cdot 1$, $v = 0, 1, 2, 3$. That means that one can write $\theta = \theta_0 \cdot \theta_1$ with $\mathrm{sw}(\theta_0) = j_v$ and $\theta_1|_{J_F U_{L_1}^t} = 1$. Thus it suffices to show

Claim". $v = 3$; i.e., $j_v = t + p^3 = 1 + p^4 + p^3$.

(From Claim" only $\mathrm{sw}(\theta) \geqq j_3$ follows. But $\mathrm{sw}(\theta)$ cannot be greater, otherwise $j(Z) = j(X)$ would be greater and thus $sw(\rho)$ would be greater as possible.) The reason for Claim" is that Z is $\mathfrak{g}$-invariant. Thus $\theta|_W$ is $\mathfrak{g}$-invariant and in particular:

> θ restricted to $(U_{L_1}^{j_v} \cap J_F U_{L_1}^t)$ is $\mathfrak{g}$-invariant and not trivial, but θ restricted to $(U_{L_1}^{j_v+1} \cap J_F U_{L_1}^t)$ becomes trivial.

Hence we can read θ as a $\mathfrak{g}$-invariant character of a subgroup of $U_{L_1}^{j_v}/U_{L_1}^{j_v+1}$. But the last group is a homogeneous $\mathbb{F}_p\mathfrak{g}$-module with irreducible submodule $V = (\mathbb{F}_p(\alpha^{j_v}), \sigma \to \alpha^{j_v})$, where α is a primitive fifth root of unity (Lemma 1.1). Since θ is $\mathfrak{g}$-invariant and one-dimensional, V must be one-dimensional too. Thus the order of α^{j_v} is a divisor of $p-1$. Since $\mathrm{ord}(\alpha) = 5$ and $p \equiv 2 \pmod 5$, it follows that $j_v \equiv 0 \pmod 5$. Thus $j_v = 1 + p^4 + p^3$. Q.E.D.

Sketch of Proof of Remark 2.2. Take the symplectic $\mathbb{F}_p\mathfrak{g}$-module $V := U_F^2/N^2$ constructed in Step 1 of the Proof of Proposition 2.1. Denote the symplectic form on V by X.

Claim. Choose any Abelian Extension M/F that has just one jump at $s = 2$ and such that $N_{M/F}U_M^2$ is maximally isotropic for X. Then one can extend X to an alternating form X' on F^* such that $N_{M/F}M^*$ is isotropic for X' and such that $j(X') = 2(1 + p^{-2})$ if and only if $d(X) = f - 2$.

Here $f = |\bar{F} : \mathbb{F}_p|$ and the definition of $d(X)$ is as follows: Identity $U_F^2/U_F^3 = \bar{F}$. Denote by τ the Frobenius of $\bar{F}/\mathbb{F}_p$. Then there is an alternating polynomial $P = \sum_{i=1}^{f-1} a_i \cdot \tau^i$ such that $X(x, y) = \mathrm{tr}_{\bar{F}/\mathbb{F}_p}(x \cdot P(y))$. (See Zink [11, Sect. 3] for the theory of alternating polynomials.) Denote by $d(X)$ the degree of P.

Since X is $\mathfrak{g}$-invariant, the degree of P is indeed $f - 2$: $\mathfrak{g}$ acts by multiplication with α^2, a fifth root of unity. Hence

$$P = \alpha^2 \cdot P \cdot \alpha^2 = \sum_{i=1}^{f-1} a_i \alpha^2 \cdot \tau^i(\alpha^2) \cdot \tau^i = \sum_{i=1}^{f-1} a_i \alpha^{2+2p^i} \cdot \tau^i.$$

Thus $a_i \neq 0$ only for those i for which $\alpha^{p^i} = \alpha^{-1}$, that is, for even i. Hence $d(x)$ is even. On the other hand, $|U_F^2 : N^2| = p^4$; thus $f > d(X) \geqq f - 2$; see [11, Sect. 4, Proposition 6 (iv)]. Since f contains fifth roots of unity and $p \equiv 2 \pmod 5$, f is even too. This implies that $d(X) = f - 2$.

The claim follows from a generalization of a result of Zink to an arbitrary jump s ([11, Sect. 3, Proposition 9]). Zink already formulated most of the steps of the proof of his Proposition 9 for general s. One just needs the right extension of his definition of $j(X)$ to extend the result of Proposition 9.

The form X' constructed in the claim is not necessarily $\mathfrak{g}$-invariant. Define a $\mathfrak{g}$-invariant form by $Y_0(x, y) := \prod_{\sigma \in \mathfrak{g}} X'(\sigma(x), \sigma(y))$. Y_0 on U_F^2 equals $X^{|\mathfrak{g}|}$. Since $|\mathfrak{g}|$ is prime to p, choose an integer c such that $c \cdot |\mathfrak{g}| \equiv 1 \pmod p$. Let $Y := Y_0^c$. Then Y is a $\mathfrak{g}$-invariant extension of X and $j(Y) \leqq 2(1 + p^{-1})$.

Assume that Y is not the form we are looking for. Then $U_1 := U_F^2 \cdot \mathrm{Rad}(Y) < F^*$, but $U_1/\mathrm{Rad}(Y)$ is Y-non-degenerate. Let U_2 be the orthogonal complement of U_1. Write $Y = Y_1 \cdot Y_2$, with $\mathrm{Rad}(Y_i) = U_i \cdot Y_1$ and Y_2 are $\mathfrak{g}$-invariant forms. Y_1 is a form with jumps $\leqq 1$. The work of Zink implies that $j(Y_1) = 1 + p^{-2}$. Y_2 is a form that has just one jump at $s = 2$. Hence $j(Y_2)$ equals $2(1 + p^{-2})$ or $2 + p^{-1}$. These conductors are all different, hence $j(Y_2) = j(Y)$. Since $j(Y)$ is small, $j(Y_2)$ is small too, and Y_2 is the form we were looking for.

References

1. J. Buhler, Icosahedral Galois representations, *in* "Springer Lecture Notes in Mathematics," Vol. 654, Springer-Verlag, Berlin/New York, 1978.
2. H. Hasse, "Number Theory," Akademie-Verlag, Berlin, 1979. [English translation]
3. G. Henniart, Representations du groupe de Weil d'un corps local, *Enseign. Math.* **26** (1980), 155–172.
4. H. Koch, Classification of the primitive representations of the Galois group of local fields, *Invent. Math.* **40** (1977), 195–216.
5. J.-P. Serre, Modular forms of weight one and Galois representations, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), Academic Press, London, 1977 (prepared in collaboration with C. Bushnell).
6. J.-P. Serre, "Local Fields," Springer-Verlag, Berlin/New York, 1979.
7. A. Turull, Supersolvable automorphism groups of solvable groups, *Math. Z.* **183** (1983), 47–73.
8. A. Weil, "Basic Number Theory," 3rd ed., Springer-Verlag, Berlin/New York, 1974.
9. E.-W. Zink, Weil-Darstellungen und lokale Galoistheorie, *Math. Nachr.* **92** (1979), 265–288.
10. E.-W. Zink, Lokale projektive Klassenkörpertheorie: Grundbegriffe und erste Resultate, Akad. d. Wiss. d. DDR, R-Math-01/82, Berlin, 1982.
11. E.-W. Zink, Lokale projektive Klassenkörpertheorie II, *Math. Nach.* **114** (1983), 123–150.